AMENDMENTS TO THE CLAIMS

The following is a complete, marked up listing of revised claims with a status identifier in parentheses, underlined text indicating insertions, and strikethrough and/or double-bracketed text indicating deletions.

LISTING OF CLAIMS:

1. (Previously Presented) An electronic data processing method method comprising:

performing a security check to ascertain a user identity by comparing entered identity information with stored user identity data;

associating the user identity with a user identifier;

associating the user identifier with at least one user group identifier;

selecting a user group identifier and acquiring at least one data key associated therewith from a centralized data store including all available keys, at least one user group identifier and at least one data key being associated with one another;

performing at least one of encrypting and decrypting data using the acquired at least one data key and inhibiting user recognition of the acquired at least one data key.

2. (Previously Presented) The method as claimed in claim 1, wherein the security check involves at least one of checking a user-specific biometric data, an electronic key and a mechanical key.

3. – 4. (Canceled)

5. (Previously Presented) The system as claimed in claim 8, wherein the data key is accessible using a data telecommunication device.

6. (Previously Presented) The method as claimed in claim 1, wherein a plurality of data keys are simultaneously assignable to one user identifier.

7. (Previously Presented) The method as claimed in claim 1, wherein the data are medically relevant, wherein the users include personnel within a medical facility, and wherein common user group identifiers are assigned the same data key.

8. (Previously Presented) An electronic data processing system comprising:

a security check device to ascertain user identity a first data store for storage and retrieval of at least one user identifier and associated user identity data;

a second data store for storage and retrieval of the at least one user identifier and associated at least one user group identifier;

a centralized third data store for storage and retrieval of all available data keys, the centralized third data store including at least one associated user group identifier matched with at least one associated data key; and

at least one processor to ascertain a user identifier by comparing data between the security check device and the first data store, to ascertain at least one user group from the second data store, to ascertain at least one data key for at least one user group from the third data store, and for performing at least one of data encryption and decryption using the at least one data key.

9. (Previously Presented) The electronic data processing system as claimed in claim 8, wherein the security check device reads biometric data from the user.

10. (Previously Presented) The electronic data processing system as claimed in claim 8, wherein the security check device is a user-specific at least one of electronic and mechanical key.

11. (Canceled).

12. (Currently Amended) The electronic data processing system as claimed in claim [[11]] 8, wherein the system uses a data telecommunication device to access the third data store.

13. (Previously Presented) The electronic data processing system as claimed in claim 8, wherein the system is a medical workstation for handling medically relevant data.

14. (Previously Presented) A computer-readable storage medium including computer executable instructions that, when executed, cause a computer to carry out the method as claimed in claim 1.

15. - 21. (Canceled).

22. (Previously Presented) A method for at least one of encryption and decryption of data, comprising:

performing a security check to ascertain an identity of a user;

associating the user with a user group including a plurality of users such that a data key for at least one of encrypting and decrypting data is assigned to the user based on the group with which the user is associated, the same data key being assignable to the plurality of users; and

at least one of encrypting or decrypting data using the assigned data key.

23. (Previously Presented) A computer-readable storage medium including computer executable instructions that, when executed, cause a computer to, carry out the method as claimed in claim 22.

24. (Original) The method as claimed in claim 22, wherein the security check involves checking biometric data of the user.

25. (Original) The method as claimed in claim 22, wherein the security check involves checking a user-specific at least one of electronic and mechanical key.

26. (Original) The method as claimed in claim 22, wherein the data key is ascertained by comparing the data obtained in the security check with content of a data key memory.

27. (Original) The method as claimed in claim 26, wherein the data obtained in the security check are compared with the content of the data key memory using a data telecommunication device.

28. (Original) The method as claimed in claim 22, wherein a plurality of data keys are simultaneously assignable to one user.

29. (Original) The method as claimed in claim 22, wherein the data are medically relevant, wherein the users include personnel at a medical facility, and wherein common user groups are assigned the same data key.

30. (Original) The method of claim 22, wherein users associated with a common user group are assigned the same data key.

31. (Previously Presented) An electronic data processing facility for at least one of encryption and decryption of data, comprising:

means for performing a security check to ascertain an identity of a user;

means for associating the user with a user group including a plurality of users a data key is assigned to the user based on the group with which the user is associated, the same data key being assignable to the plurality of users, and the data key being for at least one of encrypting and decrypting data; and

means for encrypting or decrypting data using the assigned data key.

32. (Previously Presented) The method of claim 1, wherein a user identifier associated with a common user group identifier is assigned the same data key.

33. (Previously Presented) The system of claim 8, further comprising:
A fourth data store for storage and retrieval of encrypted data.

34. (Previously Presented) The system of claim 8, wherein at least one of the first data store, the second data store and the fourth data store are combined.

35. (Previously Presented) The system of claim 8, wherein the data store comprises:

mechanical memory, electronic memory, and magnetic and optical media data storage.

36. (Previously Presented) The system of claim 8, wherein the third data store is isolated from the first, second and fourth data stores.

37. (Previously Presented) The system of claim 8, wherein data entry and retrieval is at least one of manual and automated.

38. (Previously Presented) The system of claim 12, wherein the data telecommunications device is removably and operatively associated with a computer network for transfer of data.

39. (Previously Presented) The system of claim 8, wherein the channel comprises an access and restriction process.

40. (Previously Presented) The system of claim 39, wherein the channel access and restriction process functions operatively with the security check device.